AMENDMENTS TO THE CLAIMS:

This listing of the claims will replace all prior versions, and listings, of the claims in this application.

Listing of Claims:

1. (Currently Amended) A method ~~for authorizing a network device~~, comprising:

performing an automated security scan of a second network device by a first network device to determine a capability of the second network device;

determining an attribute based, in part, on ~~a~~ the determined capability ~~of the network device~~;

generating an attribute certificate based~~,~~ in part~~,~~ on the attribute;

storing the attribute certificate including the attribute; and

responsive to a verified authentication request, determining ~~if~~ that the attribute certificate is valid~~,~~ and authorizing access to a resource over a network based, in part, on the attribute associated with the attribute certificate.

2. (Canceled).

3. (Original) The method of claim 1, wherein the attribute is further determined based, in part, on a condition to be satisfied.

4. (Original) The method of claim 1, wherein the attribute is further associated with a group of network devices.

5. (Original) The method of claim 1, wherein the attribute is further associated with a group of users.

6. (Currently Amended) The method of claim 1, wherein the attribute certificate is generated by at least one of the first network device, an access server, and an attribute authority.

7. (Currently Amended) The method of claim 1, wherein the attribute certificate is stored in at least one of the second network device, and an attribute repository.

8. (Original) The method of claim 7, wherein the attribute certificate is provided to an access server through the use of at least one of a cookie, a program, and a manual upload.

9. (Currently Amended) An apparatus ~~A network device for managing authorization to a resource over a network~~, comprising:

~~a first component~~ an interface configured to perform an automated security scan of a network device to determine a capability of the network device;

a processor configured to determine an attribute based, in part on the determined capability;

the processor further configured to generate an attribute certificate~~, wherein the attribute certificate is~~ based, in part, on ~~a~~ the attribute ~~capability of another network device~~;

a ~~second component, coupled to the first component,~~ memory configured to store the attribute certificate including the attribute; and

~~a third component, coupled to the second component,~~ responsive to a verified authentication request, the processor further configured to determine that the attribute certificate is valid and to authorize ~~the other network device to the~~ access to a resource over ~~the~~ a network based, in part, on the attribute ~~of the other network device~~ associated with the attribute certificate.

10. (Currently Amended) The ~~network device~~ apparatus of claim 9, wherein the ~~first component~~ processor is further configured to generate the attribute certificate based on a condition to be satisfied.

11. (Canceled).

12. (Currently Amended) The ~~network device~~ apparatus of ~~claim 11~~ claim 9, wherein the ~~first component~~ processor is further configured to generate the attribute certificate based on the

automated security scan of the ~~other~~ network device.

13. (Currently Amended) The ~~network device~~ apparatus of claim 9, wherein the ~~second component~~ interface is further configured to send the attribute certificate to the ~~other~~ network device to be stored~~, and the third component it further configured to receive the attribute certificate~~.

14. (Currently Amended) A ~~network~~ device for managing authorization to a resource over a network, comprising:

means to perform an automated security scan of a network device to determine a capability of the network device;

means for determining an attribute based, in part, on the determined capability of the network device;

~~a~~ means for generating an attribute certificate, wherein the attribute certificate is based in part on ~~a~~ the attribute ~~capability of another network device~~;

~~a~~ means for storing the attribute certificate; and

~~a~~ means responsive to a verified authentication request for ~~authorizing the other network device to the resource over the network based, in part, on the attribute of the other network device associated with~~ determining that the attribute certificate is valid and authorizing access to a resource over the network based, in part, on the attribute associated with the attribute certificate.

15. (New) The device of claim 14, where the means to perform an automated scan comprises an interface; and the means for determining, generating, storing, and means responsive comprises a central processing unit coupled to the interface and further coupled to a memory.

16. (New) A computer readable medium encoded with a computer program executable by a processor to perform actions comprising:

performing an automated security scan of a network device to determine a capability of the network device;

determining an attribute based, in part, on the determined capability;

generating an attribute certificate based in part on the attribute;

storing the attribute certificate including the attribute; and

responsive to a verified authentication request, determining that the attribute certificate is valid and authorizing access to a resource over a network based, in part, on the attribute associated with the attribute certificate.